Interface de commande en ligne

Cette rubrique contient les sections suivantes :

Survol de l'interface de commande en ligne

L'interface de ligne de commande (CLI) AsyncOS vous permet de configurer et de surveiller Secure Web Appliance. L'interface de ligne de commande est accessible par SSH sur les interfaces IP configurées avec ces services activés ou par un logiciel d'émulation de terminal sur le port série. Par défaut, SSH est configuré sur le port de gestion.

Les commandes sont appelées en saisissant le nom de la commande avec ou sans arguments. Si vous entrez une commande sans arguments, la commande vous invite à fournir les renseignements requis.

Accès à l'interface de commande en ligne

Vous pouvez vous connecter à l'aide de l'une des méthodes suivantes :

- **Ethernet.** Démarrez une session SSH avec l'adresse IP de Secure Web Appliance. L'adresse IP par défaut est 192.168.42.42. SSH est configuré pour utiliser le port 22.
- **Port série.** Démarrez une session de terminal avec le port de communication de votre ordinateur personnel auquel le câble série est connecté.

Premier accès

Vous pouvez ajouter d'autres utilisateurs avec des niveaux d'autorisation différents après avoir accédé à l'interface de commande en ligne pour la première fois en utilisant le compte **admin**. Pour cela, connectez-vous à l'appliance en saisissant le nom d'utilisateur et la phrase secrète par défaut **admin** :

- Nom d'utilisateur : **admin**
- Phrase secrète : **ironport**

L'Assistant de configuration du système vous invite à modifier la phrase secrète du compte **admin** la première fois que vous vous connectez avec la phrase secrète par défaut.

Vous pouvez également réinitialiser la phrase secrète du compte **admin** à tout moment à l'aide de la commande `passwd`.

Accès ultérieurs

Vous pouvez vous connecter et ouvrir une session sur l'appliance à tout moment en utilisant un nom d'utilisateur et une phrase secrète valides. Notez qu'une liste des tentatives d'accès récentes à l'appareil, réussites et échecs, pour le nom d'utilisateur actuel s'affiche automatiquement lors de la connexion.

Consultez la description de la commande `userconfig` suivante ou Administration des comptes d'utilisateur pour obtenir des renseignements sur la configuration d'utilisateurs supplémentaires.

Utilisation de l'invite de commande

L'invite de commande de niveau supérieur comprend le nom d'hôte complet, suivi du symbole supérieur à (>), suivi d'un espace. Par exemple :

```
example.com>
```

Lors de l'exécution de commandes, vous devez demander votre contribution sur l'interface de ligne de commande. Lorsque l'interface de ligne de commande attend des entrées, l'invite affiche les valeurs par défaut entre crochets (`[ ]`) suivies du symbole supérieur à (>). Lorsqu'il n'y a pas de valeur par défaut, les parenthèses sont vides.

Par exemple :

```
example.com> routeconfig

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>
```

Lorsqu'il existe un paramètre par défaut, il est affiché entre parenthèses dans l'invite de commandes. Par exemple :

```
example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection
to be interrupted when the changes are committed.
Enter new default gateway:
[172.xx.xx.xx]>
```

Lorsqu'un paramètre par défaut est affiché, taper sur la touche de retour équivaut à accepter le paramètre par défaut.

Syntaxe de la commande

En mode interactif, la syntaxe des commandes de l'interface de ligne de commande se compose de commandes uniques sans espace, sans arguments ni paramètres. Par exemple :

```
example.com> logconfig
```

Sélectionner des listes

Lorsque plusieurs choix de saisie s'affichent, certaines commandes utilisent des listes numérotées. Saisissez le numéro de la sélection à l'invite.

Par exemple :

```
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

Requêtes oui/non

Lorsqu'on doit répondre par oui ou par non, la question est posée avec une valeur par défaut entre parenthèses. Vous pouvez répondre par **Y** (O), **N**, **Yes** (Oui) ou **No** (Non). Le respect de la casse n'est pas important.

Par exemple :

```
Do you want to enable the proxy? [Y]> Y
```

Sous-commandes

Certaines commandes vous donnent la possibilité d'utiliser des directives de sous-commandes telles que `NEW`, `EDIT et DELETE`. Les fonctions `EDIT` et `DELETE` offrent une liste de valeurs précédemment configurées.

Par exemple :

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (172.xxx.xx.xx/xx: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
```

Dans les sous-commandes, appuyez sur Entrée ou Retour à une invite vide pour revenir à la commande principale.

Quitter les sous-commandes

Vous pouvez utiliser le raccourci clavier Ctrl+C à tout moment dans une sous-commande pour la quitter et retourner immédiatement au niveau supérieur de l'interface de ligne de commande.

Historique des commandes

L'interface de ligne de commande conserve un historique de toutes les commandes saisies au cours d'une session. Utilisez les flèches Haut et Bas du clavier ou les combinaisons de touches Ctrl+P et Ctrl+N pour faire défiler la liste des commandes récemment utilisées.

Commandes complémentaires

L'interface de ligne de commande d'AsyncOS prend en charge les commandes complémentaires. Vous pouvez entrer les premières lettres de certaines commandes, suivies de la touche de tabulation, et l'interface de ligne de commande complète la chaîne. Si les lettres que vous avez saisies ne sont pas uniques parmi les commandes, l'interface de ligne de commande « affine » l'ensemble. Par exemple :

```
example.com> set (press the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (pressing the Tab again completes the entry with sethostname)
example.com> sethostname
```

Validation des modifications de configuration à l'aide de l'interface CLI

- De nombreuses modifications de configuration ne prennent effet que lorsque vous les validez.
- La commande `commit` vous permet de modifier les paramètres de configuration pendant que les autres opérations se déroulent normalement.
- Pour réussir la validation des modifications, vous devez vous trouver au niveau de l'invite de commande de niveau supérieur. Tapez **Return** (Retour) dans une invite vide pour monter d'un niveau dans la hiérarchie de ligne de commande.
- Les modifications de configuration qui n'ont pas été validées sont enregistrées, mais ne prennent effet que lorsque vous exécutez la commande `commit`. Cependant, toutes les commandes ne nécessitent pas l'exécution de la commande `commit`. La sortie de la session CLI, l'arrêt du système, le redémarrage, un échec ou l'exécution de la commande `clear` efface les modifications qui n'ont pas encore été validées.
- Les modifications ne sont réellement validées que lorsque vous recevez une confirmation et un horodatage.

Commandes générales de l'interface de ligne de commande

Cette section décrit quelques commandes de base que vous pouvez utiliser dans une session CLI typique, telles que la validation et l'effacement des modifications.

Exemple d'interface de ligne de commande : validation des modifications de configuration

La saisie de commentaires après la commande de validation est facultative.

```
example.com> commit

Please enter some comments describing your changes:
[]> Changed "psinet" IP Interface to a different IP address
Changes committed: Wed Jan 01 12:00:01 2007
```

Exemple d'interface de ligne de commande : effacement des modifications de configuration

La commande clear efface toutes les modifications apportées à la configuration de l'appliance depuis la dernière commande de validation ou d'effacement.

```
example.com> clear

Are you sure you want to clear all changes since the last commit? [Y]> y
Changes cleared: Wed Jan 01 12:00:01 2007
example.com>
```

Exemple d'interface de ligne de commande : sortie de la session d'interface de commande en ligne

La commande exit vous déconnecte de l'application CLI. Les modifications de configuration qui n'ont pas été validées sont effacées.

```
example.com> exit

Configuration changes entered but not committed. Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit?  [N]> y
```

Exemple d'interface de ligne de commande : demande d'aide sur l'interface de commande en ligne

La commande `help` répertorie toutes les commandes d'interface de ligne de commande disponibles et donne une brève description de chaque commande. La commande `help` peut être appelée en tapant aide ou un seul point d'interrogation (?) dans l'invite de commande.

```
example.com> help
```

En outre, vous pouvez accéder à l'aide pour une commande spécifique en entrant **`help`** `commandname`.

Thèmes connexes

- Commandes de l'interface de ligne de commande Secure Web Appliance, on page 5

Commandes de l'interface de ligne de commande Secure Web Appliance

L'interface de ligne de commande Secure Web Appliance prend en charge un ensemble de proxy et de commandes UNIX pour accéder au système, le mettre à niveau et administrer le système.

Note Les commandes de l'interface de ligne de commande ne sont pas toutes applicables ou disponibles dans tous les modes de fonctionnement (connecteur de sécurité Web standard et infonuagique).

adminaccessconfig

Vous pouvez configurer Secure Web Appliance pour avoir des exigences d'accès plus strictes pour les administrateurs qui se connectent à l'appliance, et vous pouvez spécifier une valeur de délai d'inactivité. Reportez-vous à Paramètres de sécurité supplémentaires pour l'accès à l'appliance et à Accès au réseau de l'utilisateur pour en savoir davantage.

advancedproxyconfig

Configurez les options avancées de proxy Web; les sous-commandes sont :

`AUTHENTICATION` – Options de configuration de l'authentification :

- `When would you like to forward authorization request headers to a parent proxy` (Quand souhaitez-vous transférer les en-têtes de demande d'autorisation à un proxy parent)
- `Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog` (Entrez le domaine d'autorisation de proxy à afficher dans la boîte de dialogue d'authentification de l'utilisateur final)
- `Would you like to log the username that appears in the request URI` (Voulez-vous connecter le nom d'utilisateur qui apparaît dans l'URI de la demande?)
- `Should the Group Membership attribute be used for directory lookups in the Web UI (when it is not used, empty groups and groups with different membership attributes will be displayed)` [Si l'attribut Group Membership est utilisé pour des recherches dans l'annuaire dans l'interface utilisateur Web (lorsqu'il n'est pas utilisé, les groupes vides et les groupes avec des attributs d'appartenance différents seront affichés)]
- `Would you like to use advanced Active Directory connectivity checks?` (Voulez-vous utiliser les vérifications avancées de la connectivité Active Directory?)
- `Would you like to allow case insensitive username matching in policies?` (Voulez-vous autoriser la mise en correspondance de noms d'utilisateurs non sensible à la casse dans les politiques?)
- `Would you like to allow wild card matching with the character * for LDAP group names?` (Voulez-vous autoriser la correspondance de caractères génériques avec le caractère * pour les noms de groupe LDAP?)
- `Enter the charset used by the clients for basic authentication [ISO-8859-1/UTF-8]` (Saisissez le jeu de caractères utilisé par les clients pour l'authentification de base [ISO-8859-1/UTF-8])
- `Would you like to enable referrals for LDAP?` (Voulez-vous activer les recommandations pour LDAP?)
- `Would you like to enable secure authentication?` (Voulez-vous activer l'authentification sécurisée?)
- `Enter the hostname to redirect clients for authentication` (Saisissez le nom d'hôte pour rediriger les clients pour l'authentification)

- `Enter the surrogate timeout for user credentials` (Saisissez le délai d'expiration de substitution pour les informations d'authentification de l'utilisateur)
- `Saisissez le délai d'expiration de substitution pour les informations d'authentification de l'ordinateur`
- `Enter the surrogate timeout in the case traffic permitted due to authentication service unavailability` (Saisissez le délai d'expiration de substitution si le trafic a été autorisé en raison de l'indisponibilité du service d'authentification)
- `Enter re-auth on request denied option [disabled / embedlinkinblockpage]` [Saisissez l'option de réauthentification sur demande refusée (disabled / embedLinkinblockpage)]
- `Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication?` (Voulez-vous envoyer l'en-tête Negotiate avec l'en-tête NTLM pour l'authentification NTLMSSP?)
- `Configure username and IP address masking in logs and reports` (Configurer le masquage du nom d'utilisateur et de l'adresse IP dans les journaux et les rapports)
- `Timeout to enable/disable local Auth cache` (Délai d'expiration pour activer/désactiver le cache d'authentification local).

  Vous pouvez utiliser cette option de l'interface de ligne de commande pour activer ou désactiver le cache d'authentification immédiate du processus proxy. Le temps défini est en secondes. Par défaut, cette option est activée et définie pendant 30 secondes. Ce délai doit être plus court que le temps de substitution IP.

`CACHING` – Mode de mise en cache du proxy; choisissez une option :

- `Safe Mode` (Mode sans échec)
- `Optimized Mode` (Mode optimisé)
- `Aggressive Mode` (Mode agressif)
- `Customized Mode` (Mode personnalisé)

  Voir aussi Choix du mode de mise en mémoire cache du proxy Web.

`DNS` – Options de configuration du DNS :

- `Enter the URL format for the HTTP 307 redirection on DNS lookup failure` (Saisissez le format de l'URL pour la redirection HTTPno-break space - U+00A0307 en cas d'échec de la recherche DNS)
- `Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure?` (Voulez-vous que le proxy envoie une redirection HTTP 307 en cas d'échec de la recherche DNS?)
- `Voulez-vous que le proxy ne bascule pas automatiquement vers les résultats du DNS lorsque le proxy en amont (homologue) ne répond pas?`
- `Do you want to disable IP address in Host Header` (Voulez-vous désactiver l'adresse IP dans l'en-tête de l'hôte)
- `Find web server by:` (Trouvez un serveur Web par :)

  `0 = Always use DNS answers in order` (0=Toujours utiliser les réponses DNS dans l'ordre)

  `1 = Utiliser l'adresse fournie par le client, puis les DNS`

  `2 = Limited DNS usage` (2 = Utilisation DNS limitée)

`3 = Very limited DNS usage` (3 = Utilisation DNS très limitée)

La valeur par défaut est égale à 0. Pour les options 1 et 2, DNS sera utilisé si la réputation de sites Web est activée. Pour les options 2 et 3, les DNS seront utilisés pour les demandes de proxy explicites, s'il n'y a pas de proxy en amont ou en cas d'échec du proxy en amont configuré. Pour toutes les options, le DNS sera utilisé lorsque les adresses IP de destination sont utilisées dans l'appartenance à la politique.

`EUN` – Paramètres de notification de l'utilisateur final :

- `Choose` (Choisissez :)

  `1. Refresh EUN pages` (Actualiser les pages EUN)

  `2. Use Custom EUN pages` (Utiliser des pages EUN personnalisées)

  `3. Use Standard EUN pages` (Utiliser les pages standard EUN)

- `Would you like to turn on presentation of the User Acknowledgement page?` (Voulez-vous activer la présentation de la page de confirmation de l'utilisateur?)

Voir aussi Contrat d'utilisation du proxy Web et Survol des notifications envoyées à l'utilisateur final.

`NATIVEFTP` – Configuration FTP native :

- `Would you like to enable FTP proxy?` (Voulez-vous activer le proxy FTP?)
- `Enter the ports that FTP proxy listens on` (Saisissez les ports sur lesquels le proxy FTP écoute)
- `Enter the range of port numbers for the proxy to listen on for passive FTP connections` (Saisissez la plage de numéros de port sur laquelle le proxy doit entendre les connexions FTP passives)
- `Enter the range of port numbers for the proxy to listen on for active FTP connections` (Saisissez la plage de numéros de port sur laquelle le proxy doit entendre les connexions FTP actives)
- `Enter the authentication format :` (Entrez le format d'authentification :)

  `1. Check Point`

  `2. No Proxy Authentication` (Aucune authentification du proxy)

  `3. Raptor`

- `Would you like to enable caching?` (Voulez-vous activer la mise en cache?)
- `Would you like to enable server IP spoofing?` (Voulez-vous activer l'usurpation d'adresses IP du serveur?)
- `Would you like to enable client IP spoofing?`(Voulez-vous activer l'usurpation d'adresses IP du client?)
- `Would you like to pass FTP server welcome message to the clients?` (Voulez-vous transmettre le message de bienvenue du serveur FTP aux clients?)
- `Enter the max path size for the ftp server directory` (Entrez la taille de chemin maximale pour le répertoire du serveur FTP)

Voir aussiSurvol des services proxy FTP.

`FTPOVERHTTP` – Options FTP sur HTTP :

- `Enter the login name to be used for anonymous FTP access` (Saisissez le nom de connexion à utiliser pour l'accès FTP anonyme)
- `Enter the password to be used for anonymous FTP access` (Saisissez le mot de passe à utiliser pour l'accès FTP anonyme)

Voir aussi Survol des services proxy FTP.

`Highperformance` (Hautes performances) : active et désactive le mode haute performance.

`HTTPS` – Options liées à HTTPS :

- `HTTPS URI Logging Style - fulluri or stripquery` (Style de journalisation URI HTTPS - fulluri ou stripquery)
- `Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose?` (Voulez-vous déchiffrer les requêtes HTTPS transparentes non authentifiées à des fins d'authentification?)
- `Would you like to decrypt HTTPS requests for End User Notification purpose?` (Souhaitez-vous déchiffrer les demandes HTTPS à des fins de notification à l'utilisateur final?)
- `Action to be taken when HTTPS servers ask for client certificate during handshake:` (Action à entreprendre lorsque les serveurs HTTPS demandent un certificat client lors de l'établissement de liaison :)
  1. `Pass through the transaction` (Transmettre la transaction)
  2. `Reply with certificate unavailable` (Réponse avec certificat non disponible)
- `Do you want to enable server name indication (SNI) extension?` [Voulez-vous activer l'extension SNI (Server Name Indication)?]
- `Do you want to enable automatic discovery and download of missing Intermediate Certificates?` (Voulez-vous activer la découverte et le téléchargement automatiques des certificats intermédiaires manquants?)
- `Do you want to enable session resumption?` (Voulez-vous activer la reprise de session?)

Voir aussi Survol de la création de politiques de déchiffrement pour contrôler le trafic HTTPS.

`SCANNING` – Options d'analyse :

- `Would you like the proxy to do malware scanning all content regardless of content type` (Voulez-vous que le proxy analyse tout le contenu contre les programmes malveillants, quel que soit le type de contenu?)
- `Enter the time to wait for a response from an anti-malware scanning engine (Sophos, McAfee, or Webroot), in seconds` [Saisissez le temps d'attente d'une réponse d'un moteur d'analyse contre les programmes malveillants (Sophos, McAfee ou Webroot), en secondes]
- `Do you want to disable Webroot body scanning?` (Voulez-vous désactiver l'analyse du corps Webroot?)

Voir aussi Survol de l'analyse à la recherche de programmes malveillants et Survol de l'analyse du trafic sortant.

`SCANNERS` – Exclut les types MIME de l'analyse par le moteur Cisco Secure Endpoint . Pour utiliser la sous-commande analyseurs, vous devez désactiver la fonction de « analyse adaptative ». À l'aide de cette

sous-commande, vous pouvez ajouter les types MIME qui n'ont pas besoin d'être analysés par le moteur Cisco Secure Endpoint pour augmenter les performances d'analyse. Les options de type MIME par défaut sont « image/ALL et text/ALL ».

Pour ajouter les types MIME, vous devez les ajouter après les options par défaut. Par exemple, si vous souhaitez ajouter les types MIME vidéo et audio, le format doit être :

« image/ALL et text/ALL vidéo/ALL audio/ALL »

PROXYCONN – Gère la liste des agents utilisateurs qui ne peuvent pas accepter l'en-tête de connexion proxy. Les entrées de la liste sont interprétées comme des expressions régulières dans le langage Flex (Fast Lexical Analyzer). Un agent utilisateur sera mis en correspondance si une sous-chaîne de celui-ci correspond à une expression régulière de la liste.

- Choisissez l'opération que vous souhaitez effectuer :

  `NEW - Add an entry to the list of user agents` (NOUVEAU - Ajouter une entrée à la liste des agents utilisateurs)

  `DELETE - Remove an entry from the list` (SUPRIMER - Supprimer une entrée de la liste)

CUSTOMHEADERS – Gérer les en-têtes de demande personnalisés pour des domaines spécifiques.

- Choisissez l'opération que vous souhaitez effectuer :

  `DELETE - Delete entries` (SUPPRIMER - Supprimer des entrées)

  `NEW - Add new entries` (NOUVEAU - Ajouter de nouvelles entrées)

  `EDIT - Edit entries` (MODIFIER - Modifier les entrées)

Voir aussi Ajout d'en-têtes personnalisés aux demandes Web.

MISCELLANEOUS (DIVERS) - Paramètres divers liés au proxy :

- `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)` [Voulez-vous que le proxy réponde aux contrôles de l'intégrité des commutateurs de couche 4 (toujours activé si WSA est en mode transparent sur la couche 4)]
- `Voulez-vous que le proxy effectue un ajustement dynamique de la taille de la fenêtre de réception TCP?`
- `Would you like proxy to perform dynamic adjustment of TCP send window size?` (Voulez-vous que le proxy effectue un ajustement dynamique de la taille de la fenêtre d'envoi TCP?)
- `Do you want to filter non-HTTP responses` (Voulez-vous filtrer les réponses non HTTP?)

  `(Non-HTTP responses are filtered by default.Enter` **`N`** `if you want to allow non-HTTP responses via proxy)` (Les réponses non HTTP sont filtrées par défaut. Saisissez N si vous souhaitez autoriser les réponses non HTTP par l'intermédiaire d'un proxy)
- `Enable caching of HTTPS responses` (Activez la mise en cache des réponses HTTPS)
- `Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds)` [Saisissez le délai d'inactivité minimal pour la vérification du proxy en amont qui ne répond pas (en secondes)]
- `Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)` [Saisissez le délai d'inactivité maximal pour la vérification du proxy en amont qui ne répond pas (en secondes)]
- `Mode of the proxy:` (Mode du proxy :)

1. `Explicit forward mode only` (Mode de transfert explicite uniquement)
2. `Transparent mode with L4 Switch or no device for redirection` (Mode transparent avec commutateur de couche 4 ou aucun périphérique pour la redirection)
3. `Transparent mode with WCCP v2 Router for redirection` (Mode transparent avec routeur WCCP v2 pour la redirection)

- Usurpation de l'adresse IP du client par le proxy :
  1. `Enable for all requests` (Activer pour toutes les demandes)
  2. `Enable for transparent requests only` (Activer pour les demandes transparentes uniquement)
- `Do you want to pass HTTP X-Forwarded-For headers?` (Voulez-vous transmettre les en-têtes HTTP X-Forwarded-For?)
- `Do you want to enable server connection sharing?` (Voulez-vous activer le partage de la connexion du serveur?)
- `Would you like to permit tunneling of non-HTTP requests on HTTP ports?` (Voulez-vous autoriser la tunnellisation des requêtes non HTTP sur les ports HTTP?)
- `Would you like to block tunneling of non-SSL transactions on SSL Ports?` (Voulez-vous bloquer la tunnellisation des transactions non SSL sur les ports SSL?)
- `Voulez-vous que le proxy consigne les valeurs des en-têtes X-Forwarded-For à la place des adresses IP de connexion entrante?`
- `Do you want proxy to throttle content served from cache?` (Voulez-vous que le proxy limite le contenu servi à partir du cache?)
- `Voulez-vous que le proxy utilise les adresses IP client des en-têtes X-Forwarded-For`
- `Do you want to forward TCP RST sent by server to client?` (Voulez-vous transférer le RST du serveur TCP envoyé par le serveur au client?)
- `Voulez-vous activer la vérification de l'intégrité du proxy WCCP?`
- `Do you want to enable URL lower case conversion for velocity regex?` (Voulez-vous activer la conversion d'URL en minuscules pour l'expression régulière de vitesse?)

Voir aussi Utilisation de l'interface de données P2 pour les données de proxy Web et Configuration des paramètres du proxy Web.

`SOCKS` : options de proxy SOCKS :

- `Would you like to enable SOCKS proxy` (Voulez-vous activer le proxy SOCKS?)
- `Proxy Negotiation Timeout` (Délai d'expiration de la négociation du proxy)
- `UDP Tunnel Timeout` (Délai d'expiration du tunnel UDP)
- `SOCKS Control Ports` (Ports de contrôle SOCKS)
- `UDP Request Ports` (Ports de demande UDP)

Voir aussi Utilisation de l'interface de données P2 pour les données de proxy Web et Services proxy SOCKS.

`CONTENT-ENCODING` – Autoriser et bloquer les types de codage de contenu.

Types d'encodage de contenu actuellement autorisés : compress, deflate, gzip

Types d'encodage de contenu actuellement bloqués : S.O.

Pour modifier le paramètre d'un type d'encodage de contenu spécifique, sélectionnez une option :

1. compress

2. deflate

3. gzip

[1]>

Le type d'encodage « compress » est actuellement autorisé

Voulez-vous le bloquer? [N]>

Note La commande **centralauthcache** s'applique aux appareils compatibles avec les performances élevées et pour améliorer les performances du cache d'authentification.

adminaccessconfig

Vous pouvez configurer Secure Web Appliance pour avoir des exigences d'accès plus strictes pour les administrateurs qui se connectent à l'appliance.

configuration d'alerte

Spécifiez les destinataires des alertes et définissez les paramètres d'envoi des alertes du système.

authcache

Vous permet de supprimer une ou toutes les entrées (utilisateurs) du cache d'authentification. Vous pouvez également répertorier tous les utilisateurs actuellement inclus dans le cache d'authentification.

Note Lorsque *centralauthcache* est activé, la commande *authcache* n'affiche pas le nom d'utilisateur authentifié ISE. Pour obtenir les informations sur l'utilisateur d'ISE, utilisez la commande *isedata*.

bwcontrol

Débogue la fonctionnalité de contrôle de la bande passante.

- **bwcontrol listnips :** Affiche la liste de tous les canaux de contrôle de bande passante actifs sur Secure Web Appliance.
- **bwcontrol monitor <numéro du canal>** : pour afficher la bande passante mesurée pour le canal de transmission donné, une fois toutes les cinq secondes.

À partir d'AsyncOS 14.5, les journaux de proxy en mode Trace (Suivi) sont affichés par défaut.

Terminologie

- `URLBW` : Contrôle de la bande passante appliqué par catégorie d'URL de politique d'accès

- `OverallBW` : Contrôle de la bande passante appliqué par le quota d'activité Web globale de la politique d'accès.
- `OverallMediaBW` : Contrôle de la bande passante appliqué par la limite de bande passante globale.
- `AVCPerUserBW` : Contrôle de la bande passante appliqué par la limite de bande passante AVC.

certconfig

`SETUP` : Configure les certificats de sécurité et les clés.

`OCSPVALIDATION` : Active/désactive la validation OCSP du certificat pendant le téléchargement.

`OCSPVALIDATION_FOR_SERVER_CERT` : Active la validation OCSP pour les certificats de serveur Active la validation OCSP pour les certificats de serveur

clear

Efface les modifications de configuration en attente depuis la dernière validation.

clientconnections

Affiche les détails de la connexion lorsque le nombre maximal de connexions par client est activé. Les détails comprennent l'adresse IP du client et le nombre de connexions.

Choisissez l'opération que vous souhaitez effectuer :

- `LIST` : Répertorie toutes les entrées de la base de données de cstat
- `SEARCH` : Recherche une entrée dans la base de données de cstat

commit

Valide les modifications en attente à la configuration du système.

configbackup

Enregistre le fichier de configuration de sauvegarde et l'envoie à un serveur de sauvegarde distant par FTP ou SCP

csidconfig

Vous pouvez configurer différents paramètres de la fonctionnalité Cisco Success Network sur l'appliance en ce qui concerne la publication des données de télémesure sur le portail d'échange de services de sécurité.

Les sous-commandes sont :

- `OPT_OUT` : active/désactive la transmission des données de télémesure CSI
- `CSIDATAPUSHINTERVAL` : configure l'intervalle de temps de transmission des données de télémesure.

createcomputerobject

Crée un objet ordinateur à l'emplacement que vous spécifiez.

curl

Envoyez une demande cURL directement à un serveur Web ou à un serveur Web par l'intermédiaire d'un proxy, avec les en-têtes HTTP de demande et de réponse renvoyés pour vous permettre de déterminer la raison du chargement d'une page Web.

Note Cette commande est réservée à l'usage de l'administrateur ou de l'opérateur, sous la supervision du service d'assistance technique de Cisco.

Les sous-commandes sont :

- `DIRECT` : accès URL direct
- `APPLIANCE` : URL d'accès par le biais de l'appliance

datasecurityconfig

Définit une taille minimale de corps de demande en dessous de laquelle les demandes de téléchargement ne sont pas analysées par les filtres de sécurité des données de Cisco.

date

Affiche la date actuelle. Exemple :

```
Thu Jan 10 23:13:40 2013 GMT
```

diagnostic

Sous-commandes liées au proxy et à la création de rapports :

`NET` : utilitaire de diagnostic réseau

Cette commande est obsolète; utilisez packetcapture pour capturer le trafic réseau sur l'appliance.

`PROXY` : utilitaire de débogage de proxy

Choisissez l'opération que vous souhaitez effectuer :

- `SNAP` : prend un instantané du proxy
- `OFFLINE` : met le proxy hors ligne (par le biais de WCCP)
- `RESUME` : reprend le trafic proxy (par le biais de WCCP)
- `CACHE` : efface le cache du proxy

`proxyscannermap` : cette commande affiche le mappage de PID entre chaque proxy et le processus d'analyseur correspondant.

`REPORTING` : utilitaires de rapport

Le système de rapports est actuellement activé.

Choisissez l'opération que vous souhaitez effectuer :

- `DELETDB` : réinitialise la base de données de rapports

- `DISABLE` : désactive le système de rapports.
- `DBSTATS` : répertorie la base de données et les fichiers d'exportation (affiche la liste des fichiers et des dossiers non traités dans les dossiers export_files et always_onbox.)
- `DELETEEXPORTDB` : supprime les fichiers d'exportation (supprime tous les fichiers et dossiers non traités dans les dossiers export_files et always_onbox.)
- `DELETEJOURNAL` : supprime les fichiers de journal (supprime tous les aclog_journal_files.)

dnsconfig

Configure les paramètres du DNS.

Choisissez l'opération que vous souhaitez effectuer :

- `NEW` : ajoute un nouveau serveur.
- `EDIT` : modifie un serveur.
- `DELETE` : supprime un serveur.
- `SETUP` : configure les paramètres généraux.
- `SEARCH` : configure la liste de recherche de domaines DNS.

```
[]> setup
```

```
Do you want to enable Secure DNS? [N]> Yes
```
(Voulez-vous activer le DNS sécurisé? [N]> Oui)

dnsflush

Purge des entrées DNS sur l'appliance.

etherconfig

Configure les connexions du port Ethernet.

Choisissez l'opération que vous souhaitez effectuer :

- `MEDIA` : affiche et modifie les paramètres de supports Ethernet.
- `PAIRING` : affiche et configure l'appairage de cartes réseau.
- `VLAN` : affiche et configure les VLAN.
- `MTU` : affiche et configure la MTU.

externaldlpconfig

Définit une taille minimale de corps de demande en dessous de laquelle les demandes de téléchargement ne sont pas analysées par le serveur DLP externe.

externaldlpconfig

Définit une taille minimale de corps de demande en dessous de laquelle les demandes de téléchargement ne sont pas analysées par le serveur DLP externe.

featurekey

Soumet des clés valides pour activer les fonctionnalités sous licence.

featurekeyconfig

Vérifie et met à jour automatiquement les clés de fonctionnalité.

fipsconfig

SETUP : active/désactive la conformité FIPS 140-2 et le chiffrement des paramètres sensibles critiques (CSP). Notez qu'un redémarrage immédiat sera nécessaire.

FIPSCHECK : vérifie la conformité du mode FIPS. Indique si les divers certificats et services sont conformes aux normes FIPS.

Voir Conformité à la norme FIPS pour de plus amples informations.

grep

Recherche dans les fichiers d'entrée nommés les lignes contenant une correspondance au modèle donné.

gathererdconfig

Configure la fonctionnalité d'interrogation entre l'appliance et le serveur d'authentification.

help

Renvoie une liste de commandes.

httppatchconfig

Active ou désactive les demandes de correctifs HTTP sortantes. La valeur par défaut est enable (activer).

http2

Active ou désactive les configurations HTTP 2.

iccm_message

Efface le message de l'interface Web et de l'interface de ligne de commande indiquant quand ce Secure Web Appliance est géré par une appliance de gestion de la sécurité (Series M).

ifconfig ou interfaceconfig

Configure et gère les interfaces réseau, notamment M1, P1 et P2. Affiche les interfaces actuellement configurées et fournit un menu des opérations pour créer, modifier ou supprimer des interfaces.

iseconfig

Affiche les paramètres de configuration ISE actuels; indiquez une opération de configuration ISE à effectuer :

`ISE RECONCILIATION TIME SETUP` — Configure l'heure de rapprochement de Cisco ISE. Pour redémarrer le processus installé automatiquement, définissez l'heure au format HH::MM dans les 24 heures suivant la configuration d'ISE. Après un redémarrage, le téléchargement en bloc a lieu.

```
Choose the operation you want to perform:
- Schedule ISE Restart Time in HH:MM format.
- Modify cache timeout for ISE users. Specify a timeout value in hours, upto 24 hours
```

Par défaut, la valeur de l'option 1 est 00 h 00 à minuit.

isedata

Précisez une opération liée aux données ISE :

`statistics` : affiche l'état du serveur et les statistiques ISE du serveur.

`cache` : affiche le cache ISE ou vérifiez une adresse IP :

`sgts` : affiche le tableau des balises SGT ISE.

`groups` : affiche le tableau des groupes ISE.

Si VDI est mis en œuvre, les sous-commandes `show` et `checkip` sous la commande principale `cache` affichent plus de détails. La sous-commande `show` affiche les détails sur la plage de ports et la sous-commande `checkip` affiche les détails sur l'utilisateur VDI, tels que l'adresse IP, le nom, la plage de ports, etc.

```
[]> cache

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
```

last

Répertorie les informations utilisateur spécifiques à l'utilisateur, qui comprennent les tty et les hôtes, dans l'ordre inverse du temps ou répertorie les utilisateurs connectés à une date et à une heure spécifiées.

loadconfig

Charge un fichier de configuration système.

logconfig

Configure l'accès aux fichiers journaux.

mailconfig

Envoie le fichier de configuration actuel à l'adresse spécifiée.

maxhttpheadersize

Définit la taille maximale de l'en-tête HTTP ou la taille de l'URL pour les demandes de proxy; saisissez la valeur en octets ou ajoutez un K au nombre pour indiquer les kilo-octets.

Le suivi des politiques peut échouer pour un utilisateur qui appartient à un grand nombre de groupes d'authentification. Il peut également échouer si la taille de l'en-tête de la réponse HTTP ou la taille de l'URL est supérieure à la « taille maximale d'en-tête » actuelle. L'augmentation de cette valeur peut réduire ces échecs. La valeur minimale est de 32 Ko; la valeur par défaut est de 32 Ko; La valeur maximale est de 1 024 Ko.

modifyauthhelpers

Utilisez cette commande pour configurer le nombre d'assistants d'authentification Kerberos entre 5 et 21 pour BASIC, NTLMSSP et NEGO.

musconfig

Utilisez cette commande pour activer Secure Mobility et configurer l'identification des utilisateurs à distance, soit par adresse IP, soit par intégration dans une ou plusieurs appliances Cisco Adaptive Security Appliance.

Note Les modifications apportées à l'aide de cette commande entraînent le redémarrage du proxy Web.

musstatus

Utilisez cette commande pour afficher les informations relatives à Secure Mobility lorsque Secure Web Appliance est intégré à une appliance ASA.

Cette commande affiche les informations suivantes :

- L'état de la connexion Secure Web Appliance avec chaque appliance ASA.
- La durée de la connexion Secure Web Appliance avec chaque appliance ASA en minutes.
- Le nombre de clients distants de chaque appliance ASA.
- Le nombre de clients distants desservis, qui est défini comme le nombre de clients distants qui ont transmis du trafic par l'intermédiaire de Secure Web Appliance.
- Le nombre total de clients distants.

networktuning

Secure Web Appliance utilise plusieurs tampons et algorithmes d'optimisation pour gérer des centaines de connexions TCP simultanément, offrant des performances élevées pour le trafic Web typique, c'est-à-dire les connexions HTTP de courte durée.

Dans certaines situations, par exemple en cas de téléchargements fréquents de fichiers volumineux (plus de 100 Mo), des tampons plus grands peuvent fournir de meilleures performances par connexion. Cependant, l'utilisation globale de la mémoire augmentera et, par conséquent, toute augmentation de la mémoire tampon doit correspondre à la mémoire disponible sur le système.

Les variables d'espace d'envoi et de réception représentent les tampons utilisés pour stocker les données pour les communications sur une connexion TCP donnée. Les variables send- et received-auto sont utilisées pour activer et désactiver l'algorithme de réglage automatique de FreeBSD pour le contrôle dynamique de la taille de la fenêtre. Ces deux paramètres sont appliqués directement dans le noyau de FreeBSD.

Lorsque `SEND_AUTO` et `RECV_AUTO` sont activés, le système ajuste la taille de la fenêtre de manière dynamique en fonction de la charge du système et des ressources disponibles. Sur un Secure Web Appliance légèrement chargé, le système tente de maintenir une grande taille de fenêtre pour réduire la latence par transaction. La valeur maximale de la taille de fenêtre réglée dynamiquement dépend du nombre configuré de grappes mbuf, qui à son tour dépend de la RAM totale disponible sur le système. À mesure que le nombre total de connexions client augmente, ou lorsque les ressources de tampon réseau disponibles se raréfient, le système ajuste la taille de la fenêtre pour éviter de perdre toutes les ressources de tampon réseau à cause du trafic sur le proxy.

Consultez Problèmes de vitesse de chargement/téléchargement pour en savoir plus sur l'utilisation de cette commande.

Les sous-commandes `networktuning` sont :

SENDSPACE : Taille de la mémoire tampon de l'espace d'envoi TCP; la plage est comprise entre 8 192 et 131 072 octets; la valeur par défaut est de 16 000 octets.

RECVSPACE : Taille de la mémoire tampon de l'espace de réception TCP; la plage est comprise entre 8192 et 131072 octets; la valeur par défaut est de 32 768 octets.

SEND-AUTO : Active/désactive le réglage automatique de l'envoi TCP; 1 = activé, 0 = éteint; la valeur par défaut est désactivée. Si vous activez le réglage automatique de l'envoi TCP, veillez à utiliser `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP send window size?` (advancedproxyconfig > miscellaneous > Souhaitez-vous que le proxy effectue un réglage dynamique de la taille de la fenêtre d'envoi TCP?) pour désactiver le réglage automatique de la mémoire tampon d'envoi.

RECV-AUTO : Active/désactive le réglage automatique de la réception du protocole TCP; 1 = activé, 0 = éteint; la valeur par défaut est désactivée. Si vous activez le réglage automatique de la réception TCP, assurez-vous d'utiliser `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP receive window size?` (Souhaitez-vous que le proxy effectue un réglage dynamique de la taille de la fenêtre de réception TCP?) pour désactiver le réglage automatique de la mémoire tampon de réception.

MBUF CLUTER COUNT : Modifie le nombre de grappes mbuf disponibles; La plage de valeurs acceptables est comprise entre 98 304 et 1 572 864. La valeur doit varier en fonction de la mémoire système installée, en utilisant ce calcul : 98 304 * (X/Y) où X représente les gigaoctets de RAM sur le système et Y 4 Go. Par exemple, avec 4 Go de RAM, la valeur recommandée est 98 304 * (4/4) = 98 304. Une mise à l'échelle linéaire est recommandée à mesure que la RAM augmente.

SENDBUF-MAX : Spécifie la taille maximale de la mémoire tampon d'envoi; la plage est de 131 072 octets à 2 097 152 octets; la valeur par défaut est de 1 Mo (1 048 576 octets).

RECVBUF-MAX : Spécifiez la taille maximale de la mémoire tampon de réception; la plage est de 131 072 octets à 2 097 152 octets; la valeur par défaut est de 1 Mo (1 048 576 octets).

CLEAN-FIB-1 : Supprime toutes les entrées M1/M2 de la table de routage des données – essentiellement, activez la séparation entre le plan de contrôle et le plan de données. En d'autres termes, cela empêche tout processus du plan de données d'envoyer des données sur l'interface M1 lorsque le « routage séparé » est activé. Les processus du plan de données sont ceux pour lesquels l'option d'utilisation de la table de routage des données est activée ou qui acheminent strictement du trafic non lié à la gestion. Les processus du plan de commande peuvent toujours envoyer des données par les interfaces M1 ou P1.

Après toute modification de ces paramètres, assurez-vous de valider vos modifications et de redémarrer l'appliance.

Caution Utilisez cette commande uniquement si vous en comprenez les ramifications. Nous vous recommandons d'utiliser ce produit uniquement avec les conseils du service d'assistance technique de Cisco.

nslookup

Interroge les serveurs de noms de domaine Internet pour obtenir des renseignements à propos d'hôtes et de domaines précisés ou pour imprimer une liste des hôtes d'un domaine.

ntpconfig

Configure les serveurs NTP. Affiche les interfaces actuellement configurées et fournit un menu des opérations pour ajouter, supprimer ou définir l'interface de l'adresse IP de laquelle les requêtes NTP doivent provenir.

packetcapture

Intercepte et affiche le protocole TCP/IP et les autres paquets transmis ou reçus sur le réseau auquel l'appliance est reliée.

passwd

Définit la phrase secrète.

pathmtudiscovery

Active ou désactive Path MTU Discovery.

Vous pouvez désactiver Path MTU Discovery si vous avez besoin de la fragmentation des paquets.

ping (envoyer un message Ping)

Envoie une demande ECHO ICMP à l'hôte ou à la passerelle spécifiés.

process_status

Affiche la liste des processus actifs de l'appliance.

Note Cette commande est disponible uniquement en mode administrateur

proxyconfig <enable | disable>

Active ou désactive le proxy Web.

proxystat

Affiche les statistiques de proxy Web.

quit, q, exit

Termine un processus ou une session actif.

quotaquery

Pour vérifier ou réinitialiser le volume et l'heure utilisés par une catégorie.

Choisissez l'opération que vous souhaitez effectuer :

- `RESET` : Réinitialise le quota pour une entrée spécifique dans le cache de quota du proxy.
- `SEARCH` : Liste de recherche des entrées d'utilisateur dans le cache de quota du proxy.
- `RESETALL` : Réinitialise toutes les entrées du cache des quotas de proxy.

Note Dans un mode multi-proxy, lorsque vous souhaitez réinitialiser l'appliance tout en accédant à *quotoquery* à partir de l'interface de ligne de commande, si le nom d'utilisateur du quota se compose d'un caractère « \ », ajoutez un autre « \ », puis réinitialisez l'appliance. Par exemple, si vous trouvez un nom d'utilisateur de quota « vol:W2012-01\administrator@AD1 », avant d'effectuer une réinitialisation, modifiez-le (ajoutez « \ ») comme suit : « W2012-01\\administrator@AD1 ». Le préfixe « vol: » n'est pas requis lorsque vous effectuez une réinitialisation.

reboot (redémarrer)

Vide le cache du système de fichiers sur le disque, arrête tous les processus en cours et redémarre le système.

reportingconfig

configurer un système de rapports.

resetconfig

Rétablit les valeurs par défaut de la configuration.

revert

Rétablit une version précédente qualifiée du système d'exploitation AsyncOS pour le Web. Il s'agit d'une action très destructrice, car elle détruit tous les journaux de configuration et bases de données. Reportez-vous à Retour à une version antérieure d'AsyncOS pour le Web pour en savoir plus sur l'utilisation de cette commande.

rollbackconfig

Vous permet de restaurer l'une des 10 configurations validées précédemment. Par défaut, la fonctionnalité de configuration de restauration est activée.

rollovernow

Renouvelle un fichier journal.

routeconfig

Configure les adresses IP de destination et les passerelles pour le trafic. Affiche les routages actuellement configurés et fournit un menu des opérations pour créer, modifier, supprimer ou effacer des entrées.

saveconfig

Enregistre une copie des paramètres de configuration actuels dans un fichier. Ce fichier peut être utilisé pour restaurer les paramètres par défaut, au besoin.

Si le mode FIPS est activé, fournissez une option de gestion de la phrase secrète : `Mask passphrases` (Masquer les phrases secrètes) ou `Encrypt passphrases` (Chiffrer les phrases secrètes).

setgateway

Configure la passerelle par défaut pour l'appareil.

sethostname

Définit le paramètre de nom d'hôte.

setntlmsecuritymode

Modifie le paramètre de sécurité du domaine d'authentification NTLM pour « ads » ou « domain ».

- `domain` : AsyncOS joint le domaine Active Directory avec un compte d'approbation de sécurité de domaine. AsyncOS nécessite Active Directory pour utiliser uniquement les groupes Active Directory imbriqués dans ce mode.
- `ads` : AsyncOS rejoint le domaine en tant que membre Active Directory natif.

La valeur par défaut est `ads`.

settime

Règle l'heure du système.

settz

Affiche le fuseau horaire actuel et la version du fuseau horaire. Fournit un menu des opérations pour définir un fuseau horaire local.

showconfig

Affiche toutes les valeurs de configuration.

Note Les phrases secrètes des utilisateurs sont chiffrées.

shutdown

Met fin aux connexions et arrête le système.

smbprotoconfig

Active ou désactive la prise en charge du protocole SMB1 pour Samba version 4.11.15.

Choisissez l'opération que vous souhaitez effectuer :

- Enable (activer) : active le protocole SMB1.
- Disable (désactiver) : désactive le protocole SMB1.

smtprelay

Configure les hôtes de relais SMTP pour les courriels générés à l'interne. Un hôte de relais SMTP est nécessaire pour recevoir les courriels et les alertes générés par le système.

smtpconfig

Configure l'hôte local pour qu'il écoute les requêtes SNMP et autorise les requêtes SNMP.

sshconfig

Configure les options de nom d'hôte et de clé d'hôte pour les serveurs approuvés.

sslconfig

Le chiffrement par défaut pour AsyncOS versions 9.0 et antérieures est `Default:+kEDH`.

Le chiffrement par défaut pour les versions 9.1 à 11.8 d'AsyncOS est le suivant :

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

Dans ce cas, le chiffrement par défaut peut changer en fonction de vos sélections de chiffrement ECDHE.

Le chiffrement par défaut pour AsyncOS versions 12.0 et ultérieures est :

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

Note Mettez à jour la suite de chiffrement par défaut lors de la mise à niveau vers une version plus récente d'AsyncOS. Les suites de chiffrements ne sont pas automatiquement mises à jour. Lorsque vous effectuez une mise à niveau d'une version antérieure vers AsyncOS 12.0 ou une version ultérieure, Cisco recommande de mettre à jour la suite de chiffrement pour :

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

FALLBACK : active/désactive l'option de repli SSL/TLS. Si elle est activée, les communications avec les serveurs distants utiliseront le protocole configuré le plus bas à la suite d'un échec d'établissement de liaison.

Une fois qu'une version de protocole est négociée entre le client et le serveur, un échec de l'établissement de liaison est possible en raison de problèmes de mise en œuvre. Si cette option est activée, le proxy tente de se connecter en utilisant la version la plus basse des protocoles TLS/SSL actuellement configurés.

Note Sur les nouvelles installations d'AsyncOS 9.x, le repli est désactivé par défaut. Pour les mises à niveau de versions antérieures pour lesquelles l'option de secours existe, le paramètre actuel est conservé; Sinon, lors de la mise à niveau à partir d'une version pour laquelle l'option n'existe pas, le repli est activé par défaut.

ECDHE : active/désactive l'utilisation des chiffrements ECDHE pour LDAP.

Les chiffrements ECDH supplémentaires sont pris en charge dans les versions successives; cependant, certaines courbes nommées fournies avec certains des chiffrements supplémentaires amènent l'appliance à fermer la connexion pendant l'authentification LDAP sécurisée et le déchiffrement du trafic HTTPS. Consultez Configuration SSL pour plus d'informations sur la spécification de chiffrements supplémentaires.

Si vous rencontrez ces problèmes, utilisez cette option pour désactiver ou activer l'utilisation du chiffrement ECDHE pour l'une ou l'autre des fonctionnalités ou pour les deux.

ssltool

Exécute différentes commandes OpenSSL à partir de l'interface de ligne de commande de l'appliance pour dépanner les connexions SSL. La commande `ssltool` comprend les sous-commandes suivantes :

- **`sclient`** : il s'agit de la version d'interface de ligne de commande de la commande openssl s_client. Elle se connectera à un hôte distant à l'aide de SSL/TLS directement, sans utiliser l'appliance.
  - `COMMAND :` exécute une commande openssl s_client. Les commandes openssl s_client suivantes sont prises en charge :

    ```
    -connect, -servername, -verify, -cipher, -verify_return_error, -reconnect, -pause,
     -showcerts, -prexit, -state, -debug, -msg, -tls1, -tls1_1, -tls1_2, -no_ssl2,
    -no_ssl3, -no_tls1, -no_tls1_1, -no_tls1_2, -tlsextdebug, -no_ticket, -status,
    -save, -noout
    ```

    Consultez l'aide en ligne pour plus d'informations sur les commandes openssl s_client prises en charge.

Note Après avoir exécuté `command`, vous pouvez enregistrer le résultat dans un fichier à l'aide de l'option `-save`. Vous ne pouvez pas accéder aux fichiers journaux enregistrés. Ces fichiers journaux sont utilisés par l'équipe d'assistance de Cisco pour le débogage.

  - `HELP` : fournit des informations d'aide.

- **`CLEARLOGS`** : supprime tous les journaux générés par `ssltool`.

status

Affiche l'état du système.

supportrequest

Envoie le courriel de demande d'aide à l'assistance client de Cisco. Cela comprend les informations sur le système et une copie de la configuration principale.

(Facultatif) Si vous fournissez le numéro de la demande de service, un ensemble plus vaste d'informations sur le système et la configuration est automatiquement ajouté à la demande de service. Ces informations sont compressées et téléchargées vers la demande de service par FTP.

tail

Affiche la fin d'un fichier journal. La commande accepte le nom du fichier journal comme paramètre.

Exemple 1

```
example.com> tail
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
```

```
…
…
Enter the number of the log you wish to tail.
[]> 9
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 10:03:07 2017 Info: Begin Logfile
~
~
…
…
"CTRL-C" + "q"
```

Exemple 2

```
example.com> tail system_logs
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 09:59:10 2017 Info: Begin Logfile
…
…
"CTRL-C" + "q"
```

tcpservices

Affiche des informations sur les services TCP/IP ouverts.

techsupport

Fournit une connexion temporaire pour permettre à l'assistance client de Cisco d'accéder au système et d'aider au dépannage.

telnet

Communique avec un autre hôte à l'aide du protocole TELNET, généralement utilisé pour vérifier la connectivité.

testauthconfig

Teste les paramètres d'authentification pour un domaine d'authentification donné par rapport aux serveurs d'authentification définis dans le domaine.

testauthconfig [-d level] [nom du domaine]

L'exécution de la commande sans aucune option permet à l'appliance de répertorier les domaines d'authentification configurés parmi lesquels vous pouvez effectuer une sélection.

L'indicateur de débogage (`-d`) contrôle le niveau d'informations de débogage. Les niveaux peuvent varier entre 0 et 10. Si cela n'est pas spécifié, l'appliance utilise le niveau 0. Au niveau 0, la commande renverra une réussite ou un échec. Si les paramètres de test échouent, la commande répertorie la cause de l'échec.

Note Cisco vous recommande d'utiliser le niveau 0. N'utilisez un niveau de débogage différent que lorsque vous avez besoin d'informations plus détaillées pour le dépannage.

tuiconfig tuistatus

Ces deux commandes sont documentées dans Utilisation de l'interface de ligne de commande pour configurer les paramètres d'identification transparente avancée de l'utilisateur.

traceroute (afficher route)

Permet de suivre les paquets IP dans les passerelles et le long du chemin jusqu'à un hôte de destination.

trailblazerconfig

Vous pouvez utiliser la commande `trailblazerconfig` pour acheminer vos connexions entrantes et sortantes par les ports HTTP et HTTPS de la nouvelle interface Web.

Note Par défaut, la commande dans l'interface de ligne de commande `trailblazer` est activée sur votre appliance. Vous pouvez consulter l'aide en ligne en saisissant la commande suivante : `hello config`.

La syntaxe est la suivante :

```
trailblazerconfig enable <https_port> <http_port>

trailblazerconfig disable

trailblazerconfig status
```

Lieu :

« `enable` » exécute la commande trailblazer sur les ports par défaut (HTTPS : 4431 ou HTTP : 801).

« `disable` » met fin à la commande trailblazer.

« `status` » vérifie l'état de la commande trailblazer.

Note Si vous avez activé la commande `trailblazerconfig` sur l'appliance, l'URL de la demande contiendra le numéro de port HTTP/HTTPS ajouté au nom d'hôte.

Vous pouvez essayer l'une ou l'autre des étapes suivantes pour faciliter la navigation dans votre navigateur :

- Acceptez le certificat utilisé par l'interface Web et utilisez la syntaxe d'URL suivante : `https://hostname:<https_api_port> (par exemple, https://un.exemple.com:6443)` dans une nouvelle fenêtre de navigateur et acceptez le certificat. Ici `<https_api_port>` est le port HTTPS de l'API AsyncOS configuré dans **Network > IP Interfaces**(Réseau > Interfaces IP). Assurez-vous également que les ports API (HTTP/HTTPS) sont ouverts sur le pare-feu.
- Par défaut, la commande dans l'interface de ligne de commande `trailblazer` est activée sur votre appliance. Assurez-vous que les ports HTTP/HTTPS sont ouverts sur le pare-feu. Assurez-vous également que votre serveur DNS est capable de résoudre le nom d'hôte que vous avez spécifié pour accéder à l'appliance.

  Si la commande d'interface de ligne de commande `trailblazerconfig` est désactivée, vous pouvez exécuter la commande, vous pouvez exécuter la commande **trailblazerconfig** > **enable** à l'aide de l'interface de ligne de commande pour éviter les problèmes suivants :

  - Nécessité d'ajouter plusieurs certificats pour les ports d'API dans certains navigateurs.

- Redirection vers l'interface Web existante lorsque vous actualisez la page de mise en quarantaine des pourriels, de liste des autorisations ou de liste de blocage.
- La barre des mesures sur la page de rapport Cisco Secure Endpoint ne contient aucune donnée.

updateconfig

Configure les paramètres de mise à jour et de mise à niveau.

updatenow

Met à jour tous les composants.

upgrade

Installe la mise à niveau logicielle du système d'exploitation asynchrone.

`downloadinstall` : télécharge et installe immédiatement un pack de mise à niveau.

`download` : télécharge et enregistre le pack de mise à niveau pour l'installer ultérieurement.

Après avoir saisi l'une de ces commandes, une liste des pack de mise à niveau applicables à ce Secure Web Appliance s'affiche. Sélectionnez le pack souhaité en saisissant son numéro d'entrée, puis en appuyant sur Entrée; le téléchargement commence en arrière-plan. Pendant le téléchargement, des sous-commandes supplémentaires sont disponibles : `downloadstatus` et `canceldownload`.

Une fois le téléchargement terminé, si vous avez initialement saisi `downloadinstall`, l'installation commence immédiatement. Si vous avez entré `download`, deux commandes supplémentaires sont disponibles une fois le téléchargement terminé : `install` et `delete`. Entrez `install` pour commencer l'installation d'un pack téléchargé précédemment. Utilisez `delete` pour supprimer le pack téléchargé précédemment depuis Secure Web Appliance.

userconfig

Configure les administrateurs système.

version

Affiche des informations générales sur le système, les versions installées du logiciel système et les définitions de règles.

wccpstat

`all` : affiche les détails de tous les groupes de services WCCP (Web Cache Communication Protocol).

`servicegroup` : affiche les détails d'un groupe de services WCCP spécifique.

webcache

Examine ou modifie le contenu du cache de proxy, ou configurez des domaines et des URL que l'appliance ne met jamais en cache. Permet à un administrateur de supprimer une URL particulière du cache proxy ou de spécifier les domaines ou les URL à ne jamais stocker dans le cache proxy.

who

Affiche les utilisateurs connectés au système, pour les sessions d'interface de ligne de commande et Web.

Note Les utilisateurs individuels peuvent avoir un maximum de 10 sessions simultanées.

whoami

Affiche les informations concernant l'utilisateur.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.